ANNUAL 47 C.F.R. § 64.2009(e) CPNI Certification

EB Docket 06-36

Subject: Annual 64.2009(e) CPNI Certification for 2019, covering the prior calendar year 2018

Date Filed: February 22, 2019

Name of Company(s) Covered by this Certification:

Company Name	**Form 499 Filer ID**
Northeast Iowa Telephone Company	804732

Name of Signatory: David Byers

Title of Signatory: COO / Assistant Secretary

Certification:

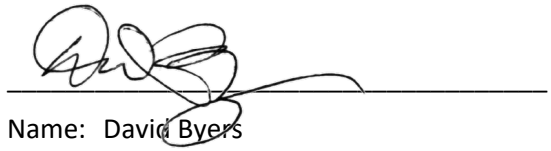
I, David Byers, acting as an agent of the company identified above, certify that I am an officer of the company and that I have personal knowledge that the company has established operating procedures that are adequate to ensure that the company is in compliance with the Commission's CPNI rules, including all requirements set forth in 47 C.F.R. § 64.2001 *et. seq.*

Attached to this certification is an accompanying statement explaining how the company's operating procedures ensure that the company is in compliance with the requirements (including those mandating the adoption of CPNI compliance policies and procedures, training, record keeping and supervisory review) set forth in 47 C.F.R. § 64.2001 *et. seq.*

The company has not taken any actions (either in proceedings instituted or petitions filed by the company with state commissions, the court system or the Commission) against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized, use, disclosure or release of CPNI.

The company represents and warrants that the above certification is consistent with 47 C.F.R. § 1.17, which requires truthful and accurate statements to the Commission. The company also acknowledges that false statements and misrepresentations to the Commission are punishable under Title 18 of the U.S. Code and may subject the companies to enforcement action.



Name: David Byers

Title: COO / Assistant Secretary

ACCOMPANYING STATEMENT

This statement accompanies the Annual 64.2009(e) CPNI Certification for 2019, covering prior calendar year 2018, filed with the Commission on behalf of Northeast Iowa Telephone Company, an Iowa corporation (the "**Company**"). The Company's operating procedures ensure that the Company is in compliance with the requirements set forth in the Commission's CPNI rules as set forth in 47 C.F.R. Part 64, Subpart U (the "**CPNI Rules**") as follows:

- The Company's operating procedures prohibit the use, disclosure or release of CPNI, except as permitted or required under 47 U.S.C. § 222(d) and Rule 64.2005. The Company does not use, disclose or permit access to CPNI for any purpose (including marketing communications-related services) and does not disclose or grant access to CPNI to any party (including to agents or affiliates that provide communications-related services), except as permitted under 47 U.S.C. § 222(d) and Rule 64.2005.

- The Company's operating procedures prohibit the use of CPNI in sales or marketing campaigns. The Company does not use, disclose or grant access to CPNI for any purpose, to any party or in any manner that would require a customer's "opt in" or "opt out" approval under the Commission's CPNI Rules. The Company does not currently solicit "opt in" or "opt out" customer approval for the use or disclosure of CPNI.

- The Company takes reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. The Company's operating procedures include safeguards designed to identify and protect against unauthorized use, disclosure or access to CPNI. The Company authenticates a customer in accordance with the Commission's CPNI rules prior to disclosing CPNI based on customer-initiated telephone contact or an in-store visit.

- The Company maintains a record of all instances where CPNI was disclosed or provided to third parties and where third parties were permitted access to CPNI. Records of all instances where CPNI was disclosed or provided to third parties, or where third parties were permitted access to CPNI, are maintained for a minimum of one year.

- The Company does not release call detail CPNI over the telephone, based on customer-initiated telephone contact, unless the customer first provides a password that is not prompted by the Company asking for readily available biographical information or account information or unless the customer is able to provide the relevant call detail information without Company assistance. If a customer does not provide a password and is not able to provide the relevant call detail information without Company assistance, the Company only discloses call detail CPNI by sending it to an address of record or by calling the customer at the telephone number of record.

- The Company provides customers with access to CPNI at the Company's retail locations only if the customer presents a valid photo ID and the valid photo ID matches an authorized name on the customer account. If a customer is not able to provide a valid photo ID, he or she may instead provide the account password in the same manner required for customer-initiated telephone contact. If a customer is not able to provide a valid photo ID or account password in connection with an in person inquiry, the Company only discloses call detail CPNI by sending it to an address of record or by calling the customer at the telephone number of record.

- The Company has established a system of passwords and password protection. For a new customer establishing service, the Company requests that the customer establish a password at the time of service initiation. For existing customers to establish a password, the Company must first authenticate the customer without the use of readily available biographical information or account information, for example by calling the customer at the telephone number of record or by using a personal identification number (PIN) or similar method to authenticate a customer.

- If a customer password is forgotten or lost, the Company uses a backup customer authentication method that is not based on readily available biographical information or account information. If a customer cannot provide a password or the proper response for the back-up authentication, the Company requires re-authentication of the customer.

- If a customer does not want to establish a password or if a password is lost or forgotten without subsequent authentication of the customer, the customer may only access call detail information based on a customer-initiated telephone call by asking the Company to send the call detail information to an address of record or by the Company calling the customer at the telephone number of record. If a customer does not want to establish a password or if a password is lost or forgotten without subsequent authentication of the customer, the customer may only access call detail information based on personal inquiry at a retail location by providing a valid photo ID that matches an authorized name on the customer account or by asking the Company to send the call detail information to an address of record or by the Company calling the customer at the telephone number of record.

- The Company has procedures and policies in place to notify a customer immediately when a password, customer response to a back-up means of authentication, address of record or other critical account information is created or changed.

- The Company does not currently provide online account access to customers.

- All Company employees with access to or a need to use CPNI have been trained regarding the Company's operating procedures and as to when they are and are not authorized to use, disclose or permit access to CPNI. The Company's employees have been trained regarding the types of information that constitute CPNI and the Company's safeguards (such as employee restrictions, password protection, supervisory review, etc.) applicable to the Company's handling of CPNI. The Company's employee manual includes a disciplinary policy requiring compliance with the Company's operating procedures and sets forth penalties for non-compliance, up to and including termination of employment.

- The Company has appointed a compliance officer and established a supervisory review process regarding the Company's compliance with the Commission's CPNI Rules. The Company's operating policies require that employees confer with the compliance officer if they are unsure about any circumstances or situations involving the potential use, disclosure or release of CPNI. The Company's operating policies require that the compliance officer confer with the Company's legal counsel if he or she is unsure about any circumstances or situations involving the potential use, disclosure or release of CPNI.

- The Company's compliance officer has personal knowledge of the Company's operating procedures and is authorized, as an agent of the Company, to sign and file an annual CPNI compliance certification with the Commission.

- All Company employees and the compliance officer are trained to identify and protect against activity that is indicative of pretexting. All Company employees and the compliance officer are required to report any breach or potential breach of CPNI safeguards and/or any customer complaints regarding CPNI. In the event of a CPNI breach, the Company's operating procedures require compliance with the Commission's CPNI Rules regarding notice to law enforcement and customers. The Company must maintain records of any discovered breaches and notifications to the Secret Service and the FBI regarding those breaches, as well as the Secret Service and the FBI responses to such notifications, for a period of at least two years.